Clock-Modulation Based Watermark for Protection of Embedded Processors

Jedrzej Kufel*, Peter Wilson*, Stephen Hill†, Bashir M. Al-Hashimi*, Paul N. Whatmough‡ and James Myers‡

*School of Electronics and Computer Science, University of Southampton, Southampton, UK
{jjk1g10,prw,bmah}@ecs.soton.ac.uk
†ARM Ltd, Austin, US, Stephen.Hill@arm.com
‡ARM Ltd, Cambridge, UK, {Paul.Whatmough,James.Myers}@arm.com

***Abstract*—This paper presents a novel watermark generation technique for the protection of embedded processors. The load circuit, reported with previous publications, responsible for the generation of particular power pattern and the majority of watermark hardware implementation costs is removed. To compensate the reduced power consumption and therefore the detection capability, we emulate the power pattern generation by reusing the existing clock gated sequential logic. The proposed technique has been validated through experiments using two ASICs in 65nm CMOS, one with an ARM Cortex-M0 microcontroller and one with a Cortex-A5 microprocessor. Silicon measurement results verify the viability of the technique for embedded processors. Furthermore, the proposed clock modulation technique demonstrates a significant area reduction, without compromising the detection performance. In our experiments the area overhead reduction of 98% was achieved. Through reuse of existing logic and reduction of watermark hardware implementation costs, the proposed clock modulation technique offers an improved robustness against removal attacks.**

***Index Terms*—Watermarking, Embedded Systems, CPA**

I. Introduction

Technology scaling and innovations in modern processes are allowing increasingly complex systems to be designed on a single die [1]. To support this design complexity it is increasingly desirable to source sub-systems, such as CPUs, from external Intellectual Property (IP) suppliers. IP blocks are usually delivered as either hard-macros, full circuit layouts, or soft-macros, typically register-transfer level (RTL) descriptions. The Virtual Socket Interface (VSI) Alliance [2] proposes three approaches to the problem of securing an IP: deterrent, protection and detection. The deterrent approach may deter the infringement from occurring through patents, copyrights, trade secrets, contracts or lawsuits [2]. However, it does not provide physical protection. The protection approach prevents unauthorized use of IP through encryption. Nonetheless, encryption and rights managements support in EDA tools is far from universal and pain-free [3]. Therefore, IP blocks are often supplied as unprotected design files that System-on-Chip (SoC) integrators can use without any complication of their design flow. As a result, auditing the presence of IP in finished products is an important challenge for IP providers. De-encapsulation and die-level reverse engineering can be used to prove the presence of IP but the process is slow and costly [3], [4]. It is therefore desirable to identify and prioritize IP candidates to be short-listed for more thorough investigation.

The VSI Alliance proposes digital watermarking as one of detection methods for physical IP protection, at various design flow levels [2]. The use of the soft IP is more desirable as it offers the end user the highest level of flexibility [2]. Methods for the protection of soft IP can be divided into two groups where architecture of the watermark circuit is closely related to the detection technique.

Watermark detection at output ports of a device through application of input vectors has been reported as one of IP protection techniques in previous work [5]–[9]. Through an addition of extra states into Finite State Machines (FSM) [5]–[7], or modification of existing states [8], [9] the area overhead of watermark implementation is reduced with a reported 0% in [9]. Nevertheless, the IP vendor may not have sufficient knowledge about the final design to able to use such detection techniques and prove the IP infringement.

In [10], Becker *et al* applied Correlation Power Analysis (CPA) [11], as a watermark detection technique. The CPA detects an embedded power watermark in the dynamic or static current variations on the supply voltage rail. Therefore, no connections to the input or output ports of a device are required. However, a power watermark requires two circuits: a watermark generator and a load circuit [10], [12]. The architecture of the watermark generation circuit depends on the watermark sequence. Nonetheless, it is kept relatively small, and 32 registers have been reported in [10], [12]. The load circuit consists of shift registers and determines the power consumed by the watermark circuit. Its size is closely related to the system size. Zeiner *et al* report 92 out of 1332 lookup tables (LUT) on FPGA, a 6.9% of system area, were used with each LUT configured as 16-bit shift register for simple arithmetic coder core [12]. Similarly, Becker *et al* utilize 16 LUTs on the AES cryptographic core [10]. It can be seen, that the majority of area overhead in the current state-of-the-art power watermark architecture is caused by the significant size load circuit.

Embedded processors are increasingly constrained in terms of circuit area. Moreover, a watermark circuit embedded in the soft IP design level is the most vulnerable to third party attacks due to high visibility of the RTL description. It is therefore

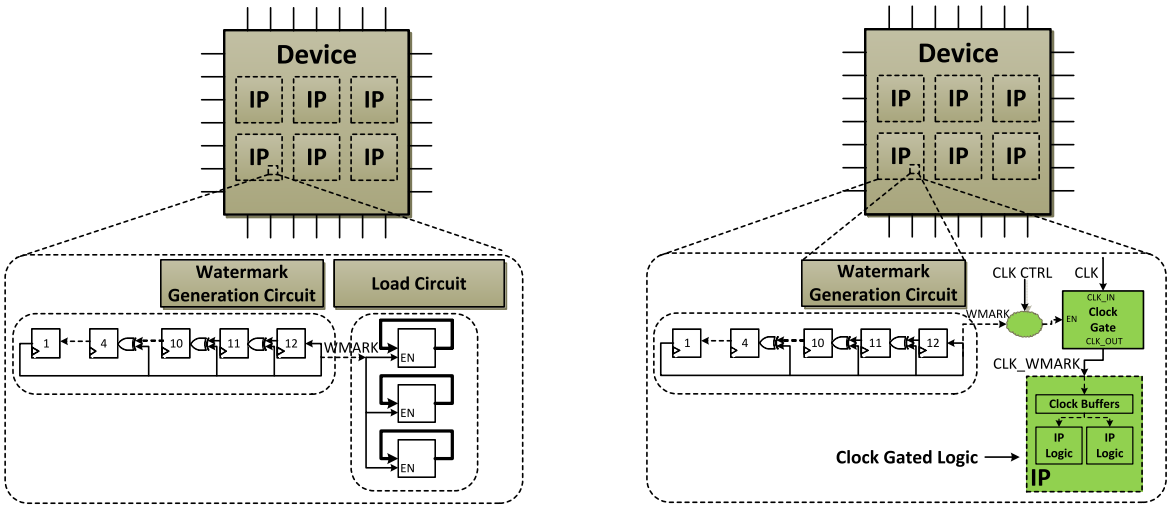


Fig. 1. Architecture of (a) current state-of-the-art, (b) proposed clock modulation power watermark circuit

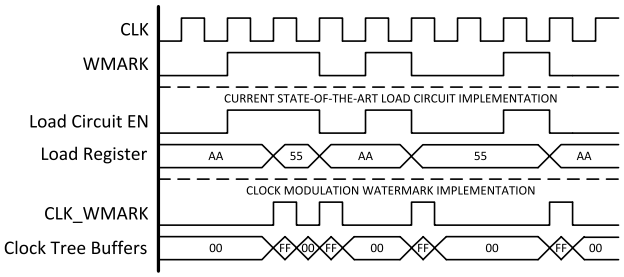


Fig. 2. Functional simulation of current state-of-the-art (middle) and clock modulation (bottom) watermark architectures

crucial for the power watermark circuit to have negligible impact on area overhead. The primary motivation of this work is therefore the minimization of power watermark hardware implementation costs, necessary for highly constrained embedded processors. In this work, we propose a novel technique to generate particular power pattern through the modulation of clock signal without compromising watermark detectability.

The paper is organized as follows. In Section II, we present the current state-of-the-art and proposed clock modulation architecture of the watermark circuit. The Correlation Power Analysis watermark detection technique is discussed in Section III. Silicon measurements are given in Section IV. Section V, discusses hardware implementation overheads. The improved robustness against removal attacks of the proposed clock modulation watermark architecture is shown in Section VI. Section VII, concludes the paper.

II. Clock Modulation Watermark Architecture

A power watermark is a redundant circuit added to an existing IP block, with the aim of superimposing a weak but deterministic signal on a supply voltage rail. The current state-of-the-art power watermark [10], [12] implements a watermark generation circuit (WGC) and a load circuit (LC), Fig. 1(a). The WGC generates the watermark sequence, $WMARK$, which controls the shift enable input of the LC. In Fig. 2, the functional simulation of the watermark circuit is shown. The load register consists of an 8-bit shift register initialized with 1010... pattern to maximize dynamic power consumption when $WMARK$ is '1'. It can be seen, that when $WMARK$ is '1' the shift enable signal is '1' and dynamic power is consumed due to shift operation during which all registers change their states. Analytical techniques such as Correlation Power Analysis (Section III), have been reported to detect deeply embedded watermark signals [10]. However, area overhead of the watermark circuit in Fig. 1(a) is significant when compared to area overhead as low as 0% with techniques [5]–[7] discussed in Section I.

To reduce area overhead we propose a technique which drives an IP sub-module with the watermark modulated clock signal as shown in Fig. 1(b). In digital circuits the distribution of a clock signal on a chip, also known as a clock tree [13], contributes to the majority of dynamic power consumption. In [14], the authors report that typically up to 50% of the total dynamic power is consumed by the system's clock signal. Since most of the processor design is sequential with a large number of registers being clocked, the fan-out of the clock tree causes high dynamic power consumption. However, not all registers must be switched every clock cycle and their state is retained for many cycles before the next update. During the clock cycles where the data is only retained and does not change an additional and redundant dynamic power is consumed due to the clock tree switching signal. To reduce the dynamic power consumption, the technique was introduced to switch off the parts of the design when it did not need to be updated. The technique is known as clock gating and requires a special clock gating logic cell to be added to the clock tree. To utilize such a high and intrinsic to the system dynamic power consumption we propose to modulate

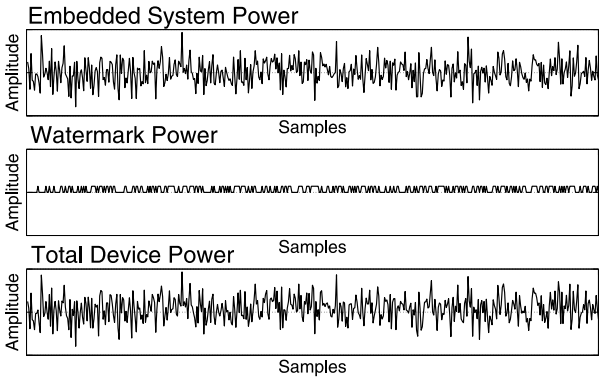


Fig. 3. Simulation results of effect of the watermark power signal on the total device power

the clock gates of an IP block. The significant size load circuit reported in previous publications [10], [12] is removed. The architecture of the WGC is the same and generates a watermark sequence, $WMARK$. The original clock gate control signal, CLK_CTRL, and $WMARK$ further control enable signal of a clock gate of an IP block, as shown in Fig. 1(b). Analogically, the original clock signal, CLK, to the IP block is modified and replaced with the modulated clock signal, CLK_WMARK. When $WMARK$ is '1', the clock gate enable is '1' and CLK is propagated, hence $CLK\_WMARK = CLK$. When $WMARK$ is '0', CLK is stopped at the clock gate and $CLK\_WMARK = 0$. In case the watermark circuit is active during processor execution, the entire IP block generates significant dynamic power in clock cycles when $WMARK$ is '1'. However, this may require an additional synchronization between the watermark modulated and other IP blocks to ensure data is not corrupted. Moreover, the size of the IP module must be significant to generate strong enough watermark power signal, due to the background noise produced by the rest of the system. In case the watermark circuit is active while the entire system is inactive, the watermark power is consumed entirely by clock tree buffers. As can be seen in Fig. 2, the clock modulation technique produces higher switching activity in comparison to watermark architecture implementing a load circuit of Fig. 1(a). This means that clock buffers switch twice in a single clock cycle during the rising and falling edges of a clock signal. Therefore the dynamic power consumed in a single register by clock tree buffers is higher than the dynamic power consumed by data switching in the same register, as shown in Section V. In Section IV, we perform experiments on silicon test chips to validate if watermark power generated in such way produces high enough amplitude to be detected with Correlation Power Analysis.

III. Watermark Detection

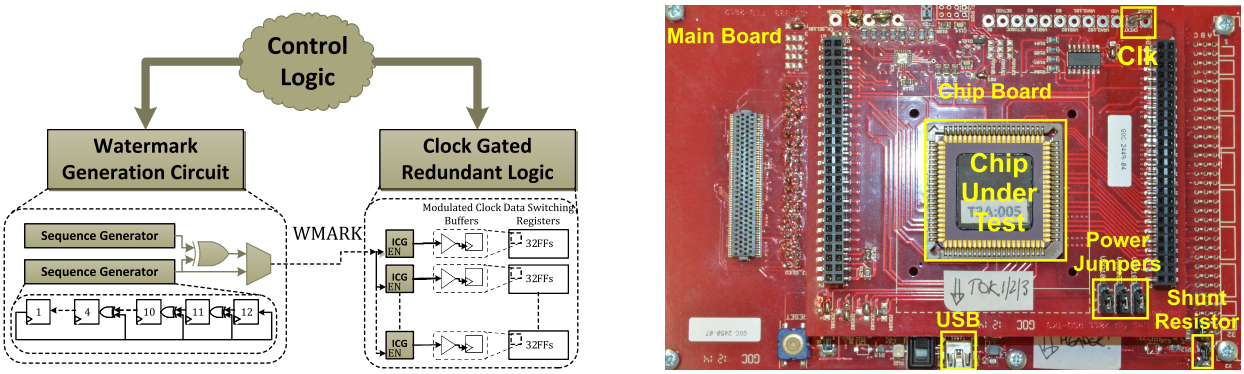
Simulation results in Fig. 3 demonstrate the effect of an additional watermark circuit on the device total power (in relative terms). The watermark power signal (middle) is added to the power consumed by the embedded system (top), and generates the device total power (bottom). Since the watermark power signal is a much lower amplitude, it is deeply embedded in the overall device power signal. We therefore require an analytical technique which determines the possibility and the accuracy of watermark existence. Such a technique is Correlation Power Analysis (CPA) [11]. It requires information extracted from the measured power consumption of a device recorded using an oscilloscope. The CPA measures the relationship between the expected (watermark sequence) and measured signals, as shown in (1).

$$\rho = \frac{N\sum_{i=1}^{N} X_i Y_i - \sum_{i=1}^{N} X_i \sum_{i=1}^{N} Y_i}{\sqrt{N\sum_{i=1}^{N} X_i^2 - (\sum_{i=1}^{N} X_i)^2}\sqrt{N\sum_{i=1}^{N} Y_i^2 - (\sum_{i=1}^{N} Y_i)^2}} \quad (1)$$

The watermark model vector, X, can be represented by a binary sequence. The sampling frequency of an oscilloscope, f_s, is much greater than the frequency of the system clock, f_{clk}, i.e. $f_s >> f_{clk}$. Hence, the measured signal is represented as vector, Y, where each value is the average of power consumed in a single clock cycle. The result is known as correlation coefficient, ρ [11]. It can vary from -1 to 1, with 1 representing two identical signals, and -1 representing two identical but inverted signals. When ρ is 0, no relationship occurs. Since both signals can be out of phase, the watermark vector X is repeatedly rotated by a single clock cycle and ρ is recalculated [10]. The number of rotations equals the period of the watermark sequence. Once all correlation values have been found, they are represented by a spread spectrum graph [10], Section IV, Fig. 5. The watermark is only regarded as detected if a single significant correlation coefficient can be resolved, as shown in Section IV, Fig. 5(a).

IV. Experimental Results

To validate proposed technique discussed in Section II, we fabricated two ASIC designs in TSMC 65nm low leakage CMOS technology, with nominal operating voltage of 1.2V. The designs were completed using industry standard EDA tools. In the first design (chip I), the watermark circuit was embedded as a hard macro block, on a separate power domain. The SoC consists of the ARM Cortex-M0 microprocessor IP core, along with an on-chip bus and numerous commercial IP blocks. In the second design (chip II), the watermark circuit was embedded from RTL description. Therefore, the watermark circuit was propagated through the entire design flow, which is closer to the intended usage scenario when embedding watermarked soft IP. The chip consists of dual core ARM Cortex-A5 microprocessor IP core and caches. The SoC consists of the ARM Cortex-M0 and the watermark circuit. The watermark circuit architecture is the same in both chips, Fig. 4(a). The WGC contains two sequence generators which can be configured as either 32-bit Linear Feedback Shift Registers or simple 32-bit circular shift registers. In our experiments, we used only a single sequence generator configured as 12-bit Linear Feedback Shift Register (LFSR), which generated 12-bit maximum length sequence at $WMARK$ output signal.



(a) (b)

Fig. 4. (a) Schematic diagram of the clock modulated watermark circuit embedded in test chips. (b) Test board

The redundant logic circuit contains 1,024 registers, divided into 32 words. The clock signal to each 32-bit word is clock gated using the clock gate cell (ICG). The clock enable signal of each clock gate cell is controlled by $WMARK$. The clock signal is propagated through all 32 clock gates when $WMARK$ is '1'. When $WMARK$ is '0', the clock signal is stopped at ICGs and no dynamic power is consumed. All registers are pre-initialized to '0', hence data switching occurs. It can be seen in Fig. 4(a), that the majority of watermark dynamic power is consumed by clock buffers embedded in registers. We can therefore validate the clock modulation technique from Section II with this experimental setup.

The test board is shown in Fig. 4(b). We connected all power domains using the power jumpers and measured the total current consumed by the chip, using the shunt $270m\Omega$ resistor. The operating frequency of both chips was 10MHz. The current signal was measured using an Agilent MSO6032A oscilloscope with Agilent 1130A active differential probe, at a sampling frequency of 500MHz. Therefore, we averaged 50 samples per single clock cycle to find the measured power vector, Y. The number of clock cycles obtained for a single ρ was 300,000. We attempted to detect the watermark while running the Dhrystone benchmark, which reflects the activities of the integer IP processor core, such as integer arithmetic, string operations, logic decisions and memory accesses in a general computing application [15], and is one of the most common benchmarks used in the industry. We executed Dhrystone benchmark on ARM Cortex-M0 on the SoC, on both chips. Although, on chip II Cortex-A5 did not execute any program both cores, along with the on-chip bus were active, which accounted for a significant portion of background noise in the system.

The spread spectra of correlation results are shown in Fig. 5. Since the period of 12-bit maximum length sequence $(2^{12}-1)$ is shorter than 300,000 clock cycles, the watermark sequence was repeated multiple times within a vector, X. It can be seen, that the correlation peak for chip I occurs at approximately the $3,800^{th}$ rotation of the watermark sequence, Fig. 5(a), and at approximately the $2,400^{th}$ rotation of the watermark sequence for chip II, Fig. 5(c). Since no other correlation peaks exist we can regard the watermark as detected. To confirm that correlation peaks were not the result of the correlated system noise, we disabled the watermark circuit and repeated experiments on both chips. As can be seen in Fig. 5(b) and Fig. 5(d), no correlation peaks occurred when watermark power pattern was not present. To investigate the repeatability of detection results we performed experiments on both chips 100 times. In Fig. 6 correlation coefficients are shown in a form of a box plot. It can be seen, that medians when X and Y were not in phase is close to 0. However, when both vectors were in phase medians are much higher and distinctive correlation peak can be distinguished. The variance of all results represented by the box in the figure accounts for 95% of all correlation coefficients with extreme values shown as dots. As can be seen, the correlation coefficient peak is present in all experiments on both chips. Therefore, an embedded watermark was successfully detected in all repetitions. The redundant logic in our experiments is a stand-alone circuit, however, in the end application a commercial IP sub-module can be reused with the same results, reducing the area overhead.

V. Area and Power Overheads

The area of the current state-of-the-art watermark circuit is greatly occupied by the significant size load circuit, as shown in Section II, Fig. 1(a). In case of system scaling, the size of the watermark generation circuit does not change, while the size of the load circuit varies and increases with the system size. This effect is caused by the Correlation Power Analysis detection technique which requires substantial watermark power signal to detect an embedded watermark circuit. Various novel detection techniques have been demonstrated in recent publications [16], [17], which detect an embedded circuit of negligible size. However, similarly to many soft IP protection techniques [5]–[9], an access to watermarked design throughout an entire design flow or access to post-fabricated design internals are necessary for successful detection. This is not possible for many IP vendors. The proposed watermark clock modulation technique enables watermark implementation at the RTL level with negligible area overhead and allows

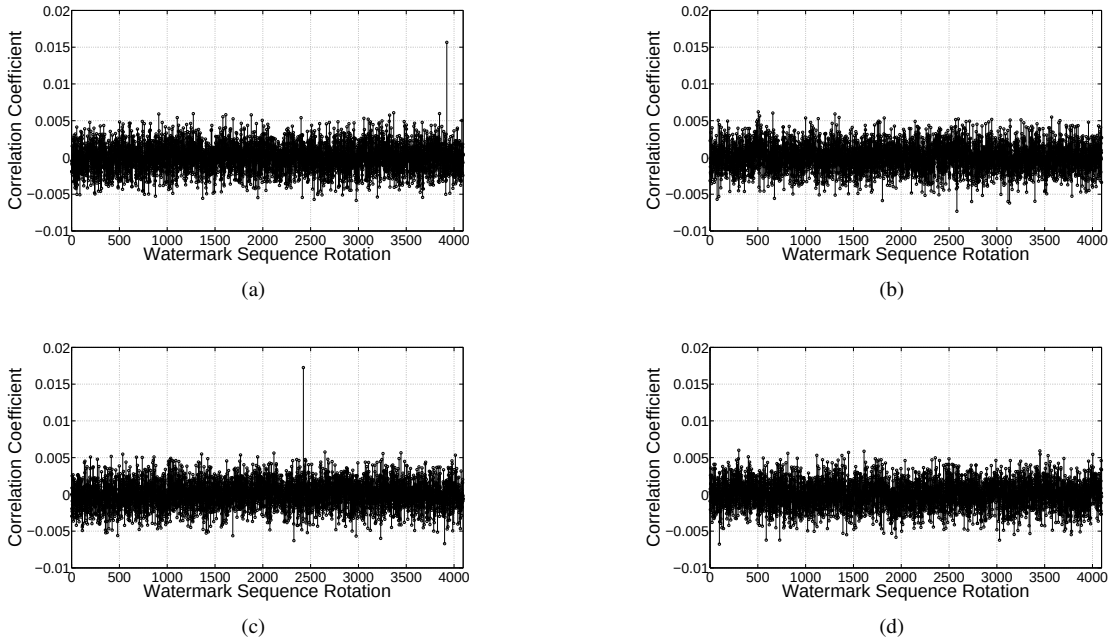


Fig. 5. Spread spectra of correlation results from test chips. Chip I with (a) active, (b) inactive, watermark circuit. Chip II with (c) active, (d) inactive watermark circuit

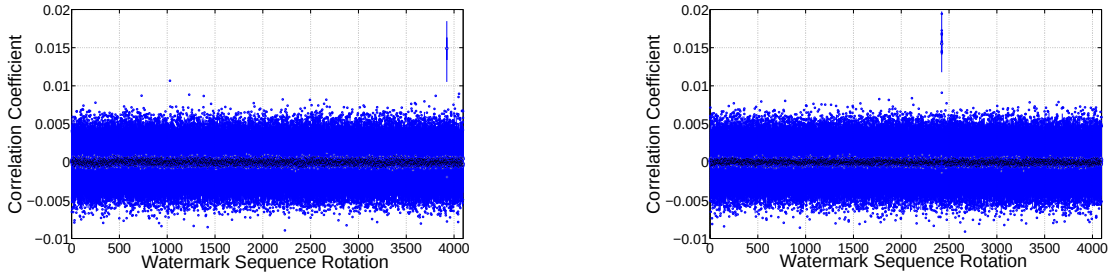


Fig. 6. Box plots of correlation coefficient results from (a) Chip I and (b) Chip II, when experiment was repeated 100 times

TABLE I
POWER CONSUMPTION OF PLACED AND ROUTED LOAD CIRCUIT

Load Circuit Implementation	**Power Consumption**			Total Watermark Dynamic Power
	Dynamic	**Static**	**Total**	
Clock Buffers Modulation No Data Switching	1.51 mW	0.404uW	1.51mW	95.6%
Clock Buffers Modulation 256 Switching Registers	1.80 mW	0.407uW	1.80mW	96.8%
Clock Buffers Modulation 512 Switching Registers	2.09 mW	0.407uW	2.09mW	97.2%
Clock Buffers Modulation 1024 Switching Registers	2.66 mW	0.408uW	2.66mW	98%

TABLE II
LOAD CIRCUIT IMPLEMENTATION COSTS

Detectable Load Circuit Dynamic Power Consumption P_{Load}	**Number of Load Circuit Registers** $N = P_{Load}/(1.126uW + 1.476uW)$	**Area Overhead Increase**
0.25 mW	96	88.9%
0.5 mW	192	94.1%
1 mW	384	96.9%
1.5 mW	576	98%
5 mW	1921	99.4%
10 mW	3843	99.7%

post-fabrication watermark detection with the CPA detection technique. Furthermore, the size of the watermark circuit is the same for all systems, hence does not need scaling, since the watermark architecture only requires implementation of the negligible size WGC.

To determine the area overhead reduction of the proposed clock modulation technique to the current state-of-the-art watermark implementation demonstrated in Section II, Fig. 1(a), we estimated the power consumption of the fully placed and routed watermark circuit, obtained with Synopsys Primetime-PX using 65nm[1] technology library. The power consumption of the clock modulated redundant load circuit is shown in

[1]TSMC 65nm low leakage technology library

Table I. In the top of the table, the load circuit is implemented as shown in Section IV, Fig. 4(a), hence the dynamic power consumption is caused entirely by clock buffers. We have found this implementation to account for 95.6% of total watermark circuit dynamic power. The number of switching registers is further increased until all 1,024 registers switch when $WMARK$ is '1'. Therefore, the dynamic power consumption is caused by both data switching and clock buffers modulation. It can be seen, that the dynamic power consumed by clock buffers is higher than the dynamic power caused by data switching. We have found that on average the dynamic power consumption of a single clock buffer is $1.476uW$, and data switching in a single register is $1.126uW$. In Table II, the number of switching registers, N, required to implement the load circuit of Section II, Fig. 1(a), is shown for various system sizes. It is based on the required load circuit dynamic power consumption (in relative terms) to be easily detected with Correlation Power Analysis. As can be seen, approximately 580 registers are required to implement the load circuit with the current state-of-the-art watermark architecture, to consume the same dynamic power as the clock gated redundant circuit in Section IV, Fig. 4(a). With the proposed clock modulation technique the dynamic power consumed by clock buffers can be obtained through the modulation of clock tree buffers of existing logic, Section II, Fig. 1(b). The watermark generation circuit requires only 12 registers, hence the area overhead reduction of 98% can be achieved. Nevertheless, the area overhead reduction depends on the system size as shown in Table II. As can be seen, the area overhead reduction is less in smaller systems, but still significant when compared to the load circuit watermark implementation. In bigger systems, the area overhead reduction is close to 100%. Moreover, watermark implementation can be system specific. Various top level IP modules or lower level sub-modules can be modulated with the proposed technique. The power overhead of the watermark implementation can be therefore tailored to the system.

VI. Improved Robustness

One of the major cornerstones of all IP watermarking techniques is the robustness against third party removal attacks. It is performed with the aim of removing watermark circuit from the design. In case of soft IP, a removal attack can be performed at the RTL description level due to high visibility of the system [2]. Since the current state-of-the-art watermark circuit implements a significant load circuit the removal is easily performed. Moreover, as the watermark is a stand-alone circuit removal has no impact on system performance.

The clock modulation technique proposed in this paper significantly reduces area overhead of the watermark circuit, leading to an enhanced robustness to removal attacks. Since, WGC can be embedded in various sub-modules detection capabilities of an attacker are significantly reduced. As can be seen in Section IV, Fig. 4(a) the proposed watermark implementation does not produce a stand-alone circuit, and therefore the system's functionality is greatly impaired when watermark is removed.

VII. Conclusions

A novel clock modulation watermark technique for embedded processors has been proposed. The technique was validated with two ASIC designs and a significant area reduction has been demonstrated when compared to the current state-of-the-art watermark circuit architecture reported in previous publications. Through embedding the watermark circuit in existing logic, the improved robustness to removal attacks was achieved.

References

[1] G. E. Moore. Cramming More Components onto Integrated Circuits. *Electronics*, 38(8):114–117, April 1965.

[2] VSI Alliance. VSI Alliance Architecture Document: Version 1.0. VSI Alliance, 1997.

[3] Intellectual Property Protection Development Working Group. Intellectual Property Protection: Schemes, Alternatives and Discussion. VSI Alliance, White Paper, August 2001.

[4] Randy Torrance and Dick James. The State-of-the-Art in IC Reverse Engineering. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, pages 363–381. Springer Berlin / Heidelberg, 2009.

[5] A.L. Oliveira. Robust Techniques For Watermarking Sequential Circuit Designs. In *Design Automation Conference, 1999. Proceedings. 36th*, pages 837–842, 1999.

[6] Ilhami Torunoglu and Edoardo Charbon. Watermarking-Based Copyright Protection of Sequential Functions. *Solid-State Circuits, IEEE Journal of*, 35(3):434–440, March 2000.

[7] Aijiao Cui, Chip-Hong Chang, Sofiene Tahar, and Amr T. Abdel-Hamid. A Robust FSM Watermarking Scheme for IP Protection of Sequential Circuit Design. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, 30(5):678–690, may 2011.

[8] Amr Abdel-Hamid, Sofiene Tahar, and El Mostapha Aboulhamid. A Public-Key Watermarking Technique for IP Designs. In *Design, Automation and Test in Europe, 2005. Proceedings*, volume 1, pages 330–335, March 2005.

[9] Amr Abdel-Hamid and Sofiene Tahar. Fragile IP Watermarking Techniques. In *Adaptive Hardware and Systems, 2008. AHS '08. NASA/ESA Conference on*, pages 513–519, June 2008.

[10] Georg Becker, Markus Kasper, Amir Moradi, and Christof Paar. Side-Channel Based Watermarks for Integrated Circuits. In *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, pages 30–35, June 2010.

[11] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis With a Leakage Model. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 135–152. Springer Berlin / Heidelberg, 2004.

[12] Daniel Ziener and Jürgen Teich. FPGA Core Watermarking Based on Power Signature Analysis. In *Field Programmable Technology, 2006. FPT 2006. IEEE International Conference on*, pages 205–212, December 2006.

[13] S. Rusu, S. Tam, H. Muljono, D. Ayers, and J. Chang. A Dual-Core Multi-Threaded Xeon Processor with 16MB L3 Cache. In *Solid-State Circuits Conference, 2006. ISSCC 2006. Digest of Technical Papers. IEEE International*, pages 315–324, February 2006.

[14] V.G. Oklobdzija, V.M. Stojanovic, D.M. Markovic, and N.M. Nedovic. *Digital System Clocking: High-Performance and Low-Power Aspects*. Wiley, 2005.

[15] Richard York. Benchmarking in context: Dhrystone. ARM, White Paper, March 2002.

[16] Xuehui Zhang and Mohammad Tehranipoor. RON: An On-Chip Ring Oscillator Network For Hardware Trojan Detection. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2011*, pages 1–6, March 2011.

[17] S. Narasimhan, D. Du, R. Chakraborty, S. Paul, F. Wolff, C. Papachristou, K. Roy, and S. Bhunia. Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis. *Computers, IEEE Transactions on*, PP(99):1, 2012.